PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-268764
(43)Date of publication of application : 09.10.1998

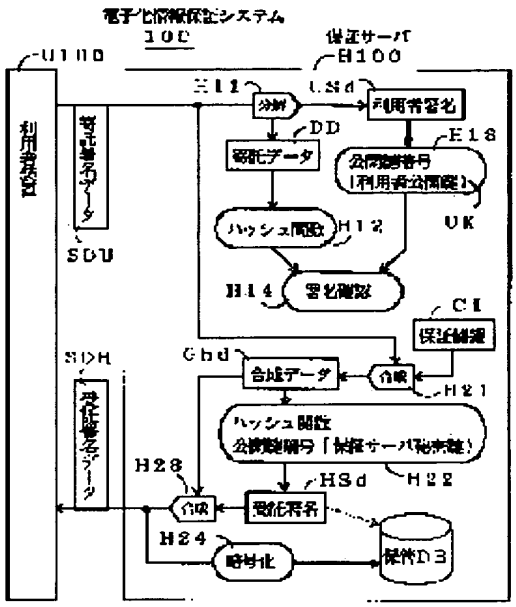
(51)Int.Cl. G09C 1/00
H04L 9/32

(21)Application number : 09-077297
(22)Date of filing : 28.03.1997

(71)Applicant : HITACHI LTD
(72)Inventor : MATSUNAGA KAZUO

(54) METHOD FOR ASSURING ELECTRONIC INFORMATION, ASSURING SERVER, AND A STORAGE MEDIUM RECORDING ASSURING SERVER PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for assuring electronic information assuring that the content of electronic information generated in the past is not altered.
SOLUTION: Electronic information in which a user electronically signed is deposited to an assuring server. The assuring server H100 adds assuring information such as time stamps, etc., to the information in which the user signed electronically. The method for ciphering is changed as necessary. Later, the user requests the assuring server H10 for a delivery of the electronic information. The assuring server H100 reads, decodes, and delivers the electronic information from a data base. Thus, it is assured by double electronic signatures of the user and the assuring server that the content is not changed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－268764

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｄ

審査請求　未請求　請求項の数７　ＯＬ　（全９頁）

(21)出願番号　特願平9－77297

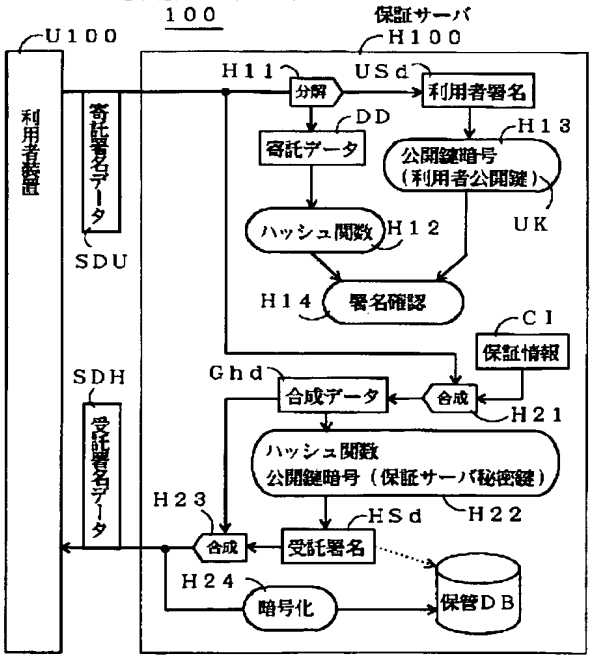
(22)出願日　平成９年(1997)３月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　松永　和男
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア開発本部
(74)代理人　弁理士　有近　紳志郎

(54)【発明の名称】　電子化情報保証方法、保証サーバおよび保証サーバプログラムを記録した記録媒体

(57)【要約】
【課題】　過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証方法を提供する。
【解決手段】　利用者が電子署名した電子化情報を保証サーバに寄託する。保証サーバは、利用者が電子署名した電子化情報にタイムスタンプなどの保証情報を付加し、電子署名し、さらに暗号化してデータベースに保管する。暗号方法は適宜変更する。後日、利用者は、電子化情報の交付を保証サーバに依頼する。保証サーバは、データベースから電子化情報を読み出し、復号し、交付する。
【効果】　利用者自身の電子署名と保証サーバの電子署名の２重の署名により、内容が変更されていないことを保証できる。

（図６）　電子化情報保証システム



1

【特許請求の範囲】

【請求項１】　利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報を保管すると共に内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することを特徴とする電子化情報保証方法。

【請求項２】　利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報のダイジェストを保管すると共に利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを利用者に保証することを特徴とする電子化情報保証方法。

【請求項３】　利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバ。

【請求項４】　利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバ。

【請求項５】　請求項３または請求項４に記載の保証サーバにおいて、前記保管手段は、電子化情報またはダイジェストを暗号化して保管すると共に、異なる暗号方式により暗号化し直して保管し直すことが可能であることを特徴とする保証サーバ。

【請求項６】　利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体。

【請求項７】　利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子化情報保証方法、保証サーバおよび保証サーバプログラムを記録した記録媒体に関し、さらに詳しくは、過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証方法、寄託された電子化情報の内容が変更されていないことを利用者に保証する保証サーバおよびその保証サーバの機能をコンピュータに実現させるための保証サーバプログラムを記録した記録媒体に関する。

2

【０００２】

【従来の技術】従来、証明機関（CertificationAuthorities）から発行された証明書を電子的に配布することにより身分を証明する身分証明技術や、作成した電子化情報に電子署名（デジタル署名）を付加することにより当該電子化情報の正当性を証明するメッセージ認証技術が知られている。しかし、過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証技術は知られていない。

【０００３】

【発明が解決しようとする課題】そこで、本発明の第１の目的は、過去に作成した電子化情報の内容が変更されていないことを保証する電子化情報保証方法を提供することにある。また、本発明の第２の目的は、寄託された電子化情報の内容が変更されていないことを利用者に保証する保証サーバを提供することにある。更に、本発明の第３の目的は、上記保証サーバの機能をコンピュータに実現させるための保証サーバプログラムを記録した記録媒体を提供することにある。

【０００４】

【課題を解決するための手段】第１の観点では、本発明は、利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報を保管すると共に内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することを特徴とする電子化情報保証方法を提供する。上記第１の観点による電子化情報保証方法では、公正な立場と認められる第三者機関が電子化情報を保管するため、内容が変更されていないことを保証して当該保管されている電子化情報を利用者に提供することが出来る。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【０００５】第２の観点では、本発明は、利用者が電子化情報を公正な立場と認められる第三者機関に寄託し、第三者機関が前記電子化情報のダイジェストを保管すると共に利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを利用者に保証することを特徴とする電子化情報保証方法を提供する。上記構成において、ダイジェストとは、電子化情報よりも情報量が少ないが電子化情報の特徴的なパターンを表した値であり、メッセージ・ダイジェストとも呼ばれる。例えば、電子化情報から一方向ハッシュ関数により作成されるハッシュ値である。上記第２の観点による

電子化情報保証方法では、公正な立場と認められる第三者機関が電子化情報のダイジェストを保管するため、利用者から保証依頼された電子化情報の内容が寄託されていた電子化情報と一致するか否かを検証できる。すなわち、内容の変更がないことを保証することが出来る。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。さらに、第三者機関は電子化情報をそのまま保管せずに、そのダイジェストを保管するため、保管の負担を軽減することが出来る。

【０００６】第３の観点では、本発明は、利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバを提供する。上記第３の観点による保証サーバを用いれば、上記第１の観点による電子化情報保証方法を好適に実施できる。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【０００７】第４の観点では、本発明は、利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とを具備することを特徴とする保証サーバを提供する。上記第４の観点による保証サーバを用いれば、上記第２の観点による電子化情報保証方法を好適に実施できる。よって、例えば契約書を電子化して寄託しておけば、当事者が保有している契約書の内容が契約後に改竄されていないことを何時でも確認できるようになり、取引の安全性を確保できるようになる。

【０００８】第５の観点では、本発明は、上記第３または第４の観点により保証サーバにおいて、前記保管手段は、電子化情報またはダイジェストを暗号化して保管すると共に異なる暗号方式により暗号化し直して保管し直すことが可能であることを特徴とする保証サーバを提供する。上記第５の観点による保証サーバでは、電子化情報またはダイジェストを暗号化して保管するため、保管中に内容が改竄されてしまうことを防止できる（どこを改竄すればよいか判らなくなる）。また、現在使用している暗号方式の解読方法が発見されてしまう可能性があるが、解読方法が発見されていない暗号方式により暗号化し直して保管し直すことが可能であるため、安全性を確保することが出来る。

【０００９】第６の観点では、本発明は、利用者から寄託された電子化情報を保管する保管手段と、保管していた電子化情報とその内容が変更されていないことの電子化保証とを含む電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。上記第６の観点による記録媒体に記録された保証サーバプログラムをコンピュータに読み取らせれば、上記第３の観点による保証サーバを実現できる。

【００１０】第７の観点では、本発明は、利用者から寄託された電子化情報のダイジェストを生成し保管する保管手段と、利用者から保証依頼された電子化情報のダイジェストを生成し前記保管していたダイジェストと照合し一致したときに内容が変更されていないことを保証する電子化保証書を発行する電子化保証書発行手段とをコンピュータに実現させる保証サーバプログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。上記第７の観点による記録媒体に記録された保証サーバプログラムをコンピュータに読み取らせれば、上記第４の観点による保証サーバを実現できる。

【００１１】

【発明の実施の形態】以下、図に示す本発明の実施形態により本発明をさらに説明する。なお、これにより本発明が限定されるものではない。

【００１２】－第１の実施形態－

図１は、保証サーバＨ１００が、社会的に信用のある証明サーバＣ１００から、保証サーバ証明書ＨＣと証明サーバ公開鍵ＣＫとを受け取る作業の説明図である。保証サーバＨ１００は、証明サーバＣ１００に対して、必要な書類（法人登記簿など）と保証サーバ情報（保証サーバ名称など）ＨＩと保証サーバ公開鍵ＨＫとを渡して、保証サーバ証明書ＨＣの発行を申請する。証明サーバＣ１００は、保証サーバ情報ＨＩと保証サーバ公開鍵ＨＫとを合成して合成情報Ｇｈｃを作成する（Ｃ１）。次に、その合成情報Ｇｈｃからハッシュ関数を用いてハッシュ値を算出し、証明サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して証明サーバ署名ＣＳｈを作成する（Ｃ２）。次に、合成情報Ｇｈｃと証明サーバ署名ＣＳｈを合成し（Ｃ３）、保証サーバ証明書ＨＣを作成し、保証サーバＨ１００に渡す。同時に、証明サーバ公開鍵ＣＫも保証サーバＨ１００に渡す。

【００１３】図２は、利用者装置Ｕ１００が証明サーバＣ１００から利用者証明書ＵＣと証明サーバ公開鍵ＣＫとを受け取る作業の説明図である。利用者装置Ｕ１００は、証明サーバＣ１００に対して、必要な書類と利用者情報（利用者名称など）ＵＩと利用者公開鍵ＵＫとを渡して、利用者証明書ＵＣの発行を申請する。証明サーバＣ１００は、利用者情報ＵＩと利用者公開鍵ＵＫとを合成して合成情報Ｇｕｃを作成する（Ｃ１１）。次に、その合成情報Ｇｕｃからハッシュ関数を用いてハッシュ値を算出し、証明サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して証明サーバ署名ＣＳｕを作成す

る（Ｃ１２）。次に、合成情報Ｇｕｃと証明サーバ署名ＣＳｕを合成し（Ｃ１３）、利用者証明書ＵＣを作成し、利用者装置Ｕ１００に渡す。同時に、証明サーバ公開鍵ＣＫも利用者装置Ｕ１００に渡す。

【００１４】図３は、利用者装置Ｕ１００が保証サーバＨ１００に接続する作業の説明図である。利用者装置Ｕ１００と保証サーバＨ１００とにより電子化情報保証システム１００が構成されている。保証サーバＨ１００の機能は、保証サーバプログラムを記録した記録媒体をコンピュータが読み込んで実現する。同様に、利用者装置Ｕ１００もコンピュータであり、利用者装置Ｕ１００と保証サーバＨ１００とは通信回線で接続されている。利用者装置Ｕ１００は、保証サーバＨ１００に対して接続要求Ｒｃを送り、保証サーバＨ１００から応答として返されてくる保証サーバ証明書ＨＣを受け取る。次に、保証サーバ証明書ＨＣを合成情報Ｇｈｃと証明サーバ署名ＣＳｈに分解し（Ｕ１）、合成情報Ｇｈｃからハッシュ関数によりハッシュ値を求め（Ｕ２）、証明サーバ署名ＣＳｈを証明サーバ公開鍵ＣＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ３）、２つのハッシュ値を照合して証明サーバＣ１００の署名を確認する（Ｕ４）。証明サーバＣ１００の署名が確認できたら、合成情報Ｇｈｃを保証サーバ情報ＨＩと保証サーバ公開鍵ＨＫとに分解する（Ｕ５）。証明サーバＣ１００の署名が確認できなければ、処理を打ち切る（以下、同様）。次に、保証サーバ情報ＨＩを確認し（Ｕ６）、誤りがなければ利用者証明書ＵＣを保証サーバＨ１００に送る。誤りがあれば処理を打ち切る（以下、同様）。

【００１５】図４は、保証サーバＨ１００が利用者装置Ｕ１００の接続を受け入れる作業の説明図である。保証サーバＨ１００は、利用者装置Ｕ１００から接続要求Ｒｃを受け取ると、応答として保証サーバ証明書ＨＣを返す。次に、利用者装置Ｕ１００から送られてくる利用者証明書ＵＣを受け取る。次に、利用者証明書ＵＣを合成情報Ｇｕｃと証明サーバ署名ＣＳｕに分解し（Ｈ１）、合成情報Ｇｕｃからハッシュ関数によりハッシュ値を求め（Ｈ２）、証明サーバ署名ＣＳｕを証明サーバ公開鍵ＣＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ３）、２つのハッシュ値を照合して証明サーバＣ１００の署名を確認する（Ｈ４）。証明サーバＣ１００の署名が確認できたら、合成情報Ｇｕｃを利用者情報ＵＩと利用者公開鍵ＵＫとに分解する（Ｈ５）。次に、利用者情報ＵＩを確認し（Ｈ６）、誤りがなければ利用者装置Ｕ１００の接続を受け入れる。

【００１６】図５は、利用者装置Ｕ１００が保証サーバＨ１００に電子化情報（以下、寄託データという）を寄託する作業の説明図である。利用者装置Ｕ１００は、寄託データＤＤからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名ＵＳｄを作成する（Ｕ１２）。次に、寄託データＤＤと利用者署名ＵＳｄを合成し（Ｕ１３）、寄託署名データＳＤＵを作成し、保証サーバＨ１００に送る。次に、保証サーバＨ１００から応答として返されてくる受託署名データＳＤＨを受け取る。次に、受託署名データＳＤＨを合成データＧｈｄと受託署名ＨＳｄに分解し（Ｕ２１）、合成データＧｈｄからハッシュ関数によりハッシュ値を求め（Ｕ２２）、受託署名ＨＳｄを保証サーバ公開鍵ＨＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ２３）、２つのハッシュ値を照合して保証サーバＨ１００の署名を確認する（Ｕ２４）。保証サーバＨ１００の署名が確認できたら、合成データＧｈｄを保証情報（受託時のタイムスタンプなど）ＣＩと寄託署名データＳＤＵとに分解する（Ｕ２５）。保証サーバＨ１００の署名が確認できなければ、処理を打ち切る（以下、同様）。次に、保証情報ＣＩを確認する（Ｕ２６）。また、分解して得た寄託署名データＳＤＵが送ったものと一致するか照合する（Ｕ２７）。さらに、受託署名ＨＳｄを保存しておく（Ｕ２８）。

【００１７】図６は、保証サーバＨ１００が利用者装置Ｕ１００からの寄託データＤＤを保管する作業の説明図である。保証サーバＨ１００は、利用者装置Ｕ１００から送られてくる寄託署名データＳＤＵを受け取る。次に、寄託署名データＳＤＵを寄託データＤＤと利用者署名ＵＳｄに分解し（Ｈ１１）、寄託データＤＤからハッシュ関数によりハッシュ値を求め（Ｈ１２）、利用者署名ＵＳｄを利用者公開鍵ＵＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ１３）、２つのハッシュ値を照合して利用者の署名を確認する（Ｈ１４）。利用者の署名が確認できなければ、処理を打ち切る（以下、同様）。利用者の署名が確認できたら、寄託署名データＳＤＵと保証情報ＣＩとを合成し、合成データＧｈｄを作成する（Ｈ２１）。次に、合成データＧｈｄからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して受託署名ＨＳｄを作成する（Ｈ２２）。次に、合成データＧｈｄと受託署名ＨＳｄを合成して、受託署名データＳＤＨを作成する（Ｈ２３）。そして、受託署名データＳＤＨを利用者装置Ｕ１００に送ると共に、内部的に用いる暗号方式により暗号化し且つ受託署名ＨＳｄと対応付けて保管ＤＢに保管する。なお、定期的または不定期的に、その時に解読方法が事実上発見されていない最新の暗号方式により暗号化し直し、保管し直す。

【００１８】図７は、利用者装置Ｕ１００が保証サーバＨ１００に保証書ＩＣの交付を依頼する作業の説明図である。利用者装置Ｕ１００は、保存していた受託署名ＨＳｄからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名ＵＳｉを作成する（Ｕ３２）。次に、受託署名ＨＳｄと利用者署名ＵＳｉを合成し（Ｕ３

３）、交付依頼Ｒｉを作成し、保証サーバＨ１００に送る。次に、保証サーバＨ１００から応答として返されてくる保証書ＩＣを受け取る。次に、保証書ＩＣを合成データＧｈｉと保証署名ＨＳｉに分解し（Ｕ４１）、合成データＧｈｉからハッシュ関数によりハッシュ値を求め（Ｕ４２）、保証署名ＨＳｉを保証サーバ公開鍵ＨＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ４３）、２つのハッシュ値を照合して保証サーバＨ１００の署名を確認する（Ｕ４４）。保証サーバＨ１００の署名が確認できたら、合成データＧｈｉを交付情報（交付時のタイムスタンプなど）ＩＩと受託署名データＳＤＨとに分解する（Ｕ４５）。次に、受託署名データＳＤＨを合成データＧｈｄと受託署名ＨＳｄに分解する（Ｕ４６）。次に、合成データＧｈｄを保証情報ＣＩと寄託署名データＳＤＵとに分解する（Ｕ４７）。次に、寄託署名データＳＤＵを寄託データＤＤと利用者署名ＵＳｄに分解する（Ｕ４８）。かくして、利用者は、内容に変更がないことを保証サーバＨ１００が保証した寄託データＤＤを得ることが出来る。なお、利用者は、自己の利用者署名ＵＳｄがあるため、内容に変更がない旨の保証サーバＨ１００の保証を否定することは出来ない。

【００１９】図８は、保証サーバＨ１００が利用者装置Ｕ１００に保証書ＩＣを交付する作業の説明図である。保証サーバＨ１００は、利用者装置Ｕ１００から送られてくる交付依頼Ｒｉを受け取る。次に、交付依頼Ｒｉを受託署名ＨＳｄと利用者署名ＵＳｉに分解し（Ｈ３１）、受託署名ＨＳｄからハッシュ関数によりハッシュ値を求め（Ｈ３２）、利用者署名ＵＳｉを利用者公開鍵ＵＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ３３）、２つのハッシュ値を照合して利用者の署名を確認する（Ｈ４４）。利用者の署名が確認できたら、受託署名ＨＳｄをキーとして保管ＤＢを検索し、対応するデータを取り出し、内部的に用いる暗号方式により復号化して受託署名データＳＤＨを得る（Ｈ３５）。次に、受託署名データＳＤＨと交付情報ＩＩとを合成し、合成データＧｈｉを作成する（Ｈ４１）。次に、合成データＧｈｉからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して保証署名ＨＳｉを作成する（Ｈ４２）。次に、合成データＧｈｉと保証署名ＨＳｉを合成して、保証書ＩＣを作成する（Ｈ４３）。そして、保証書ＩＣを利用者装置Ｕ１００に送る。

【００２０】以上の第１の実施形態の電子化情報保証システム１００によれば、過去に作成した電子化情報（寄託データＤＤ）の内容が変更されていないことを保証サーバＨ１００が利用者（Ｕ１００）に保証することが出来る。

【００２１】なお、上記第１の実施形態では、利用者装置Ｕ１００から保証サーバＨ１００への接続作業と寄託作業とを順に行ったが、次の第２の実施形態で説明するように同時に行ってもよい。

【００２２】－第２の実施形態－

利用者装置Ｕ２００と保証サーバＨ２００とにより電子化情報保証システム２００が構成されている。保証サーバＨ２００の機能は、保証サーバプログラムを記録した記録媒体をコンピュータが読み込んで実現する。同様に、利用者装置Ｕ２００もコンピュータであり、利用者装置Ｕ２００と保証サーバＨ２００とは通信回線で接続されている。図９は、利用者装置Ｕ２００が保証サーバＨ２００に接続すると同時に電子化情報（以下、寄託データという）を寄託する作業の説明図である。Ｕ１２～Ｕ１３は、図５のＵ１２～Ｕ１３と同じであり、寄託データＤＤからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名ＵＳｄを作成し（Ｕ１２）、寄託データＤＤと利用者署名ＵＳｄを合成し（Ｕ１３）、寄託署名データＳＤＵを作成する。次に、寄託署名データＳＤＵと利用者証明書ＵＣとを合成し（Ｕ５１）、証明寄託署名データＸＤを作成し、保証サーバＨ２００に送る。次に、保証サーバＨ２００から応答として返されてくる証明受託署名データＹＤを受け取る。次に、証明受託署名データＹＤを受託署名データＳＤＨと保証サーバ証明書ＨＣに分解する（Ｕ６１）。Ｕ１～Ｕ５は、図３のＵ１～Ｕ６と同じであり、保証サーバ証明書ＨＣを合成情報Ｇｈｃと証明サーバ署名ＣＳｈに分解し（Ｕ１）、合成情報Ｇｈｃからハッシュ関数によりハッシュ値を求め（Ｕ２）、証明サーバ署名ＣＳｈを証明サーバ公開鍵ＣＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ３）、２つのハッシュ値を照合して証明サーバＣ１００の署名を確認し（Ｕ４）、合成情報Ｇｈｃを保証サーバ情報ＨＩと保証サーバ公開鍵ＨＫとに分解し（Ｕ５）、保証サーバ情報ＨＩの内容を確認する（Ｈ６）。Ｕ２１～Ｕ２８は、図５のＵ２１～Ｕ２８と同じであり、受託署名データＳＤＨを合成データＧｈｄと受託署名ＨＳｄに分解し（Ｕ２１）、合成データＧｈｄからハッシュ関数によりハッシュ値を求め（Ｕ２２）、受託署名ＨＳｄを保証サーバ公開鍵ＨＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ２３）、２つのハッシュ値を照合して保証サーバＨ２００の署名を確認し（Ｕ２４）、合成データＧｈｄを保証情報（受託時のタイムスタンプなど）ＣＩと寄託署名データＳＤＵとに分解し（Ｕ２５）、保証情報ＣＩを確認し（Ｕ２６）、分解して得た寄託署名データＳＤＵが送ったものと一致するか照合し（Ｕ２７）、受託署名ＨＳｄを保存しておく（Ｕ２８）。さらに、合成データＧｈｄを保存しておく（Ｕ６８）。

【００２３】図１０は、保証サーバＨ２００が利用者装置Ｕ２００の接続を許可すると共に寄託データＤＤのハッシュ値を暗号化して保管する作業の説明図である。保証サーバＨ２００は、利用者装置Ｕ２００から送られて

くる証明寄託署名データＸＤを寄託署名データＳＤＵと利用者証明書ＵＣに分解する（Ｈ５１）。Ｈ１～Ｈ６は、図４のＨ１～Ｈ６と同じであり、利用者証明書ＵＣを合成情報Ｇｕｃと証明サーバ署名ＣＳｕに分解し（Ｈ１）、合成情報Ｇｕｃからハッシュ関数によりハッシュ値を求め（Ｈ２）、証明サーバ署名ＣＳｕを証明サーバ公開鍵ＣＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ３）、２つのハッシュ値を照合して証明サーバＣ１００の署名を確認し（Ｈ４）、合成情報Ｇｕｃを利用者情報ＵＩと利用者公開鍵ＵＫとに分解し（Ｈ５）、利用者情報ＵＩを確認し（Ｈ６）、誤りがなければ利用者装置Ｕ２００の接続を許可する。Ｈ１１～Ｈ１４は、図６のＨ１１～Ｈ１４と同じであり、寄託署名データＳＤＵを寄託データＤＤと利用者署名ＵＳｄに分解し（Ｈ１１）、寄託データＤＤからハッシュ関数によりハッシュ値を求め（Ｈ１２）、利用者署名ＵＳｄを利用者公開鍵ＵＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ１３）、２つのハッシュ値を照合して利用者の署名を確認する（Ｈ１４）。Ｈ２１～Ｈ２３は、図６のＨ２１～Ｈ２３と同じであり、寄託署名データＳＤＵと保証情報ＣＩとを合成し、合成データＧｈｄを作成し（Ｈ２１）、合成データＧｈｄからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して受託署名ＨＳｄを作成し（Ｈ２２）、合成データＧｈｄと受託署名ＨＳｄを合成して、受託署名データＳＤＨを作成する（Ｈ２３）。次に、合成データＧｈｄからハッシュ関数を用いてハッシュ値を算出し（Ｈ５７）、内部的に用いる暗号方式により暗号化し（Ｈ５８）、受託署名ＨＳｄと対応付けて保管ＤＢに保管する。なお、定期的または不定期的に、その時に解読方法が事実上発見されていない最新の暗号方式により暗号化し直し、保管し直す。さらに、受託署名データＳＤＨと保証サーバ証明書ＨＣとを合成し（Ｈ５９）、証明受託署名データＹＤを作成して利用者装置Ｕ２００に送る。

【００２４】図１１は、利用者装置Ｕ２００が保証サーバＨ２００に寄託データＤＤの内容が変更されていないことの保証を依頼する作業の説明図である。利用者装置Ｕ２００は、保存していた受託署名ＨＳｄと合成データＧｈｄとを合成し（Ｕ７１）、保証依頼データＧｖｄを作成する。次に、保証依頼データＧｖｄからハッシュ関数を用いてハッシュ値を算出し、利用者秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して利用者署名ＵＳｖを作成する（Ｕ７２）。次に、保証依頼データＧｖｄと利用者署名ＵＳｖを合成し（Ｕ７３）、保証依頼ＶＤを作成し、保証サーバＨ２００に送る。次に、保証サーバＨ２００から応答として返されてくる保証結果ＶＲを受け取る。次に、保証結果ＶＲを合成情報Ｇｈｖと保証署名ＨＳｖに分解し（Ｕ８１）、合成情報Ｇｈｖからハッシュ関数によりハッシュ値を求め（Ｕ８２）、保証

署名ＨＳｖを保証サーバ公開鍵ＨＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｕ８３）、２つのハッシュ値を照合して保証サーバＨ２００の署名を確認する（Ｕ８４）。保証サーバＨ２００の署名が確認できたら、合成情報Ｇｈｖを交付情報ＩＩと照合結果Ｒとに分解する（Ｕ８５）。かくして、利用者は、内容に変更がないことを保証サーバＨ２００が保証した照合結果Ｒを得ることが出来る。

【００２５】図１２は、保証サーバＨ２００が利用者装置Ｕ２００に保証結果ＶＲを交付する作業の説明図である。保証サーバＨ２００は、利用者装置Ｕ２００から送られてくる保証依頼ＶＤを受け取る。次に、保証依頼ＶＤを保証依頼データＧｖｄと利用者署名ＵＳｖに分解し（Ｈ８１）、保証依頼データＧｖｄからハッシュ関数によりハッシュ値を求め（Ｈ８２）、利用者署名ＵＳｖを利用者公開鍵ＵＫを用いた公開鍵暗号により復号化してハッシュ値に戻し（Ｈ８３）、２つのハッシュ値を照合して利用者の署名を確認する（Ｈ８４）。利用者の署名が確認できたら、保証依頼データＧｖｄを合成データＧｈｄと受託署名ＨＳｄに分解する（Ｈ８５）。次に、合成データＧｈｄからハッシュ関数によりハッシュ値を求める（Ｈ８６）。また、受託署名ＨＳｄをキーとして保管ＤＢを検索し、対応するデータを取り出し、内部的に用いる暗号方式により復号化してハッシュ値を得る（Ｈ８７）。次に、合成データＧｈｄから求めたハッシュ値と復号したハッシュ値を照合し（Ｈ８８）、照合結果Ｒを作成する。次に、照合結果Ｒと交付情報ＩＩとを合成し、合成情報Ｇｈｖを作成する（Ｈ９１）。次に、合成情報Ｇｈｖからハッシュ関数を用いてハッシュ値を算出し、保証サーバ秘密鍵を用いた公開鍵暗号によりハッシュ値を暗号化して保証署名ＨＳｖを作成する（Ｈ９２）。次に、合成情報Ｇｈｖと保証署名ＨＳｖを合成して、保証結果ＶＲを作成する（Ｈ９３）。そして、保証結果ＶＲを利用者装置Ｕ２００に送る。

【００２６】以上の第２の実施形態の電子化情報保証システム２００によれば、過去に作成した寄託データＤＤの内容が変更されていないことを保証サーバＨ２００が利用者装置Ｕ２００に保証することが出来る。さらに、保証サーバＨ２００は、寄託データＤＤをそのまま保管せずに、そのハッシュ値を保管するため、保管の負担を軽減することが出来る。

【００２７】なお、上記第２の実施形態では、利用者装置Ｕ２００から保証サーバＨ２００への接続作業と寄託作業とを同時に行ったが、先述した第１の実施形態で説明したように順に行ってもよい。

【００２８】

【発明の効果】本発明の電子化情報保証方法によれば、過去に作成した電子化情報の内容が変更されていないことを公正な第三者機関が保証するため、取引の安全性を確保できるようになる。また、本発明の保証サーバによ

れば、寄託された電子化情報の内容が変更されていないことを利用者に保証することが出来る。更に、本発明の保証サーバプログラムを記録した記録媒体によれば、上記保証サーバの機能をコンピュータに実現させることが出来る。

【図面の簡単な説明】

【図１】保証サーバが証明サーバから保証サーバ証明書と証明サーバ公開鍵とを受け取る作業の説明図である。

【図２】利用者装置が証明サーバから利用者証明書と証明サーバ公開鍵とを受け取る作業の説明図である。

【図３】利用者装置が保証サーバに接続する作業の説明図である。

【図４】保証サーバが利用者装置の接続を受け入れる作業の説明図である。

【図５】利用者装置が保証サーバに電子化情報を寄託する作業の説明図である。

【図６】保証サーバが利用者装置からの寄託データを保管する作業の説明図である。

【図７】利用者装置が保証サーバに保証書の交付を依頼する作業の説明図である。

【図８】保証サーバが利用者装置に保証書を交付する作業の説明図である。

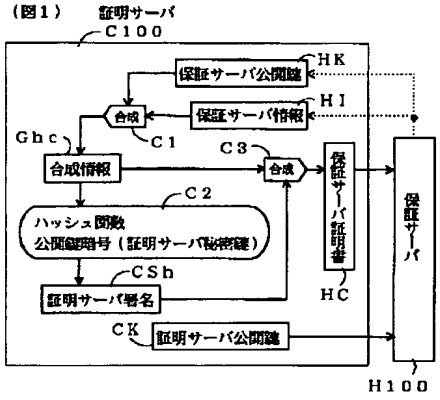
【図９】利用者装置が保証サーバに接続すると同時に電子化情報を寄託する作業の説明図である。

【図１０】保証サーバが利用者装置の接続を許可すると共に寄託データのハッシュ値を暗号化して保管する作業の説明図である。

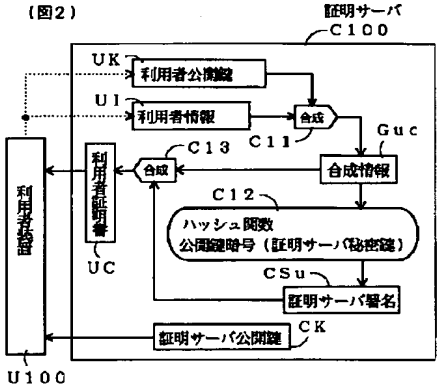
【図１１】利用者装置が保証サーバに寄託データの内容が変更されていないことの保証を依頼する作業の説明図である。

【図１２】保証サーバが利用者装置に保証結果を交付する作業の説明図である。

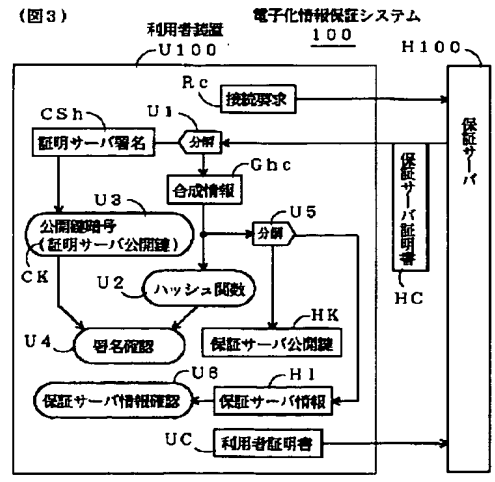
【図１】



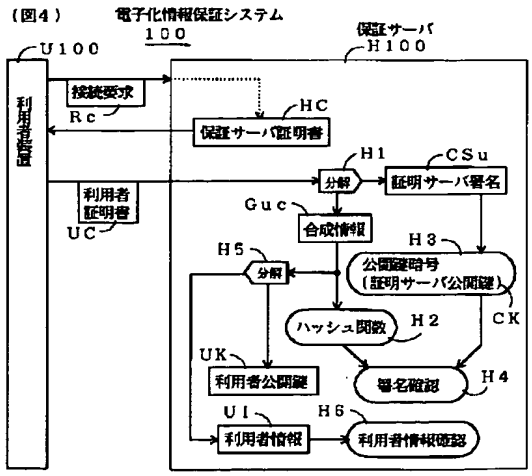
【図２】



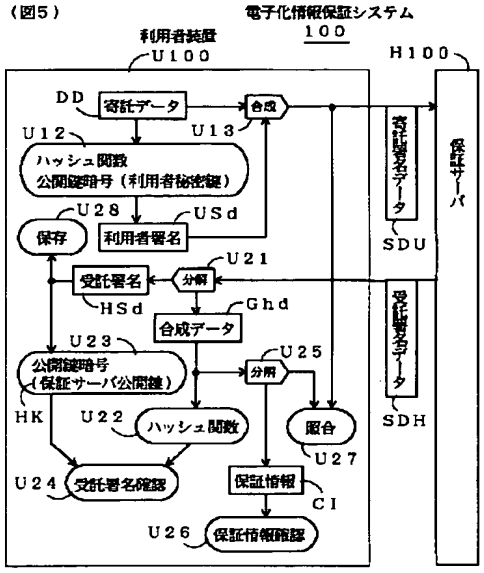
【図３】



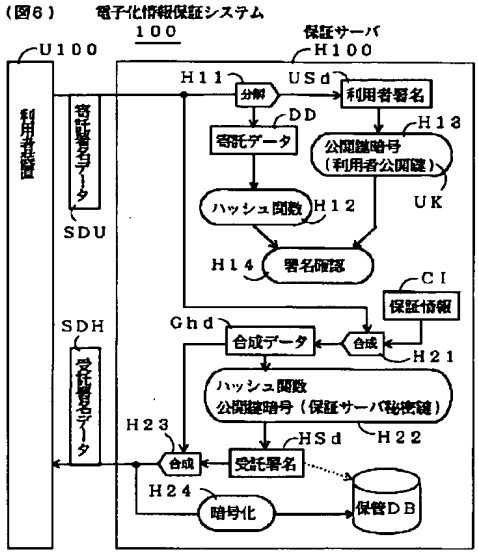
【図４】



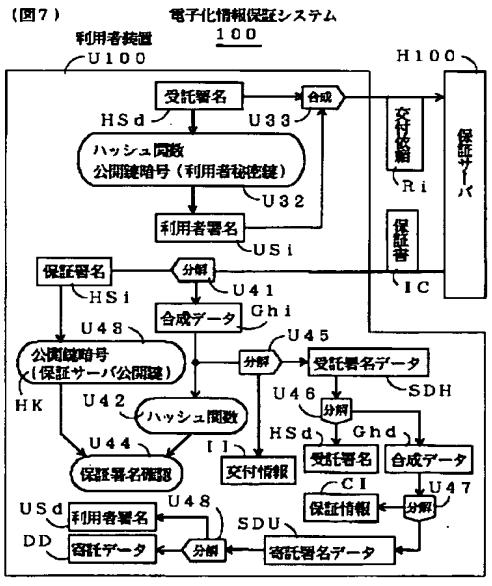
【図５】



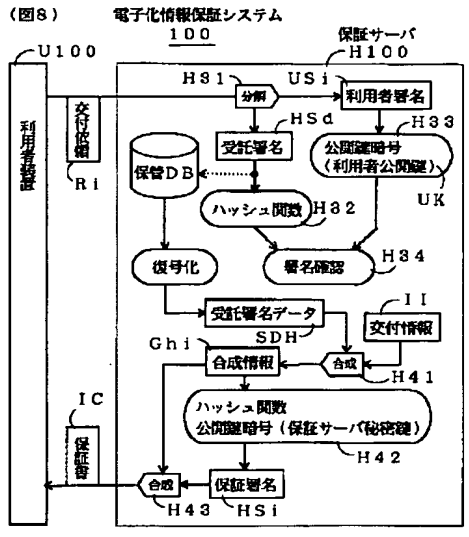
【図６】



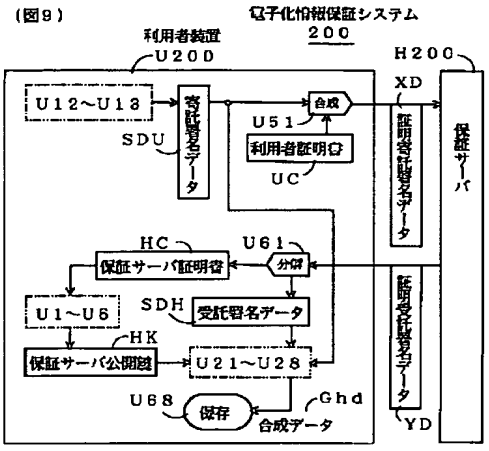
【図７】



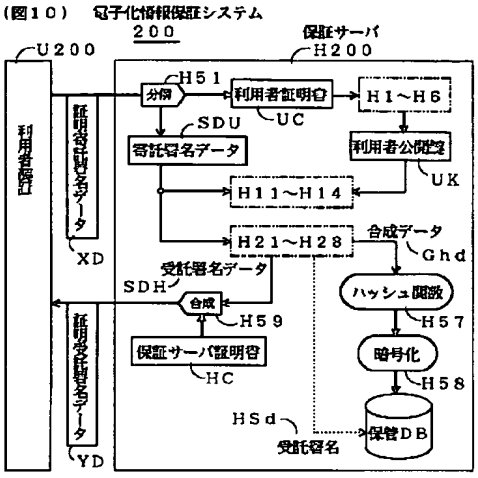
【図８】



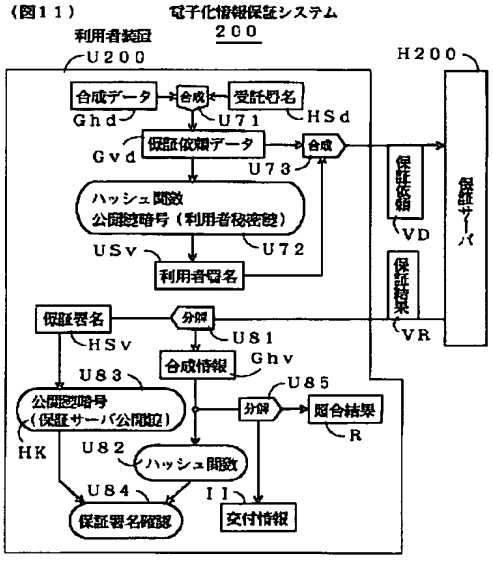
【図９】



【図１０】



【図１１】



【図１２】